ZyXEL

ZLD 2.20 Introduction

For ZyWALL USG series

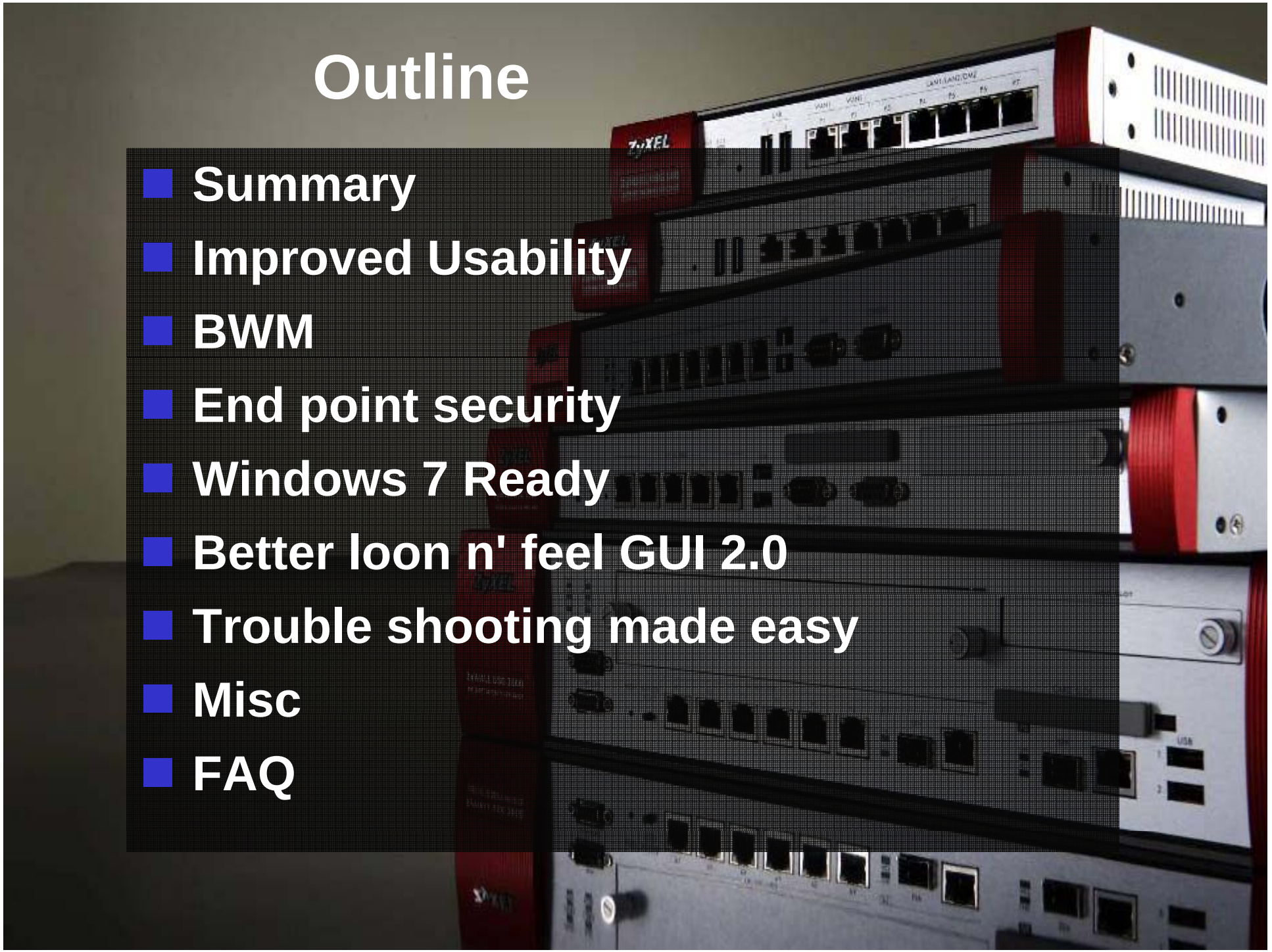
ZyXEL Communications Corp.

Date : 2009/08/11

Connecting the Future !

Celebrating our Two Decades ! ZyXEL

Outline



- Summary
- Improved Usability
- BWM
- End point security
- Windows 7 Ready
- Better loon n' feel GUI 2.0
- Trouble shooting made easy
- Misc
- FAQ

Summary: (1/2)

ZLD v2.20 Main Features	
Improved Usability	***What improved?***
ZLD packet flow v2.0	Auto disable policy route rule when next-hop is dead
	User do not need to setup policy route for default LAN to WAN traffic
	User do not need to setup policy route for IPSec Traffic
	Policy Route overwrite all routing, event
	Support Many 1 to 1 NAT
	Support Outgoing Many to Many overload NAT
Unified Interface design	Consistent all USG interface configuration style
Object reference	Object Reference look up: Display “Where used” for each objects
CF enhancement	Bypass CF check on IPSec VPN
BWM	***What improved?***
DSCP	Diff SERV tagging
	BWM by DSCP mark
End point security	***What improved?***
EPS (with SSL VPN)	End point security check against SSLVPN
EPS (with Authentication Policy)	Support Kaspersky AV client (AV enforcer)
Windows 7 ready	***What improved?***
SSLVPN enhancement	SSLVPN full tunnel supports Windows 7

Summary: (2/2)

ZLD v2.20 Main Features	
Better look n' feel	***What improved?***
GUI v2.0	Using Web 2.0 (Ajax) technology; much more flexible and easy-to-use
	Virtual device on dashboard
Trouble shooting made easy	***What improved?***
GUI v2.0 (Better loon n' feel)	Log display support for source/destination interface and protocol
	Packet Capture configuration on GUI
	Control packet capturing from GUI.
	Supports multiple interfaces capture simultaneously.
	Download pcaps from GUI.
Misc	***What improved?***
AAA enhancement	Support LDAP User Group
Authentication Policy	Enhanced version of force user authentication
3G enhancement	More 3G card support (USB) & 3G budget control
IPSec VPN enhancement	IPSec HA Auto Fall Back (ZyNOS-alike feature)
HA enhancement	Support Bridge/VLAN on Device HA AP mode
SIP ALG enhancement	SIP ALG 1.2: Support IPPBX in DMZ zone scenario
DNS query method	Device DNS query bind with specific interface.
Routing enhancement	RIP/OSPF on VLAN

Improved Usability

- ZLD packet flow 2.0
- CF enhancement
- Object reference

Celebrating our Two Decades !

Problem on current ZLD design

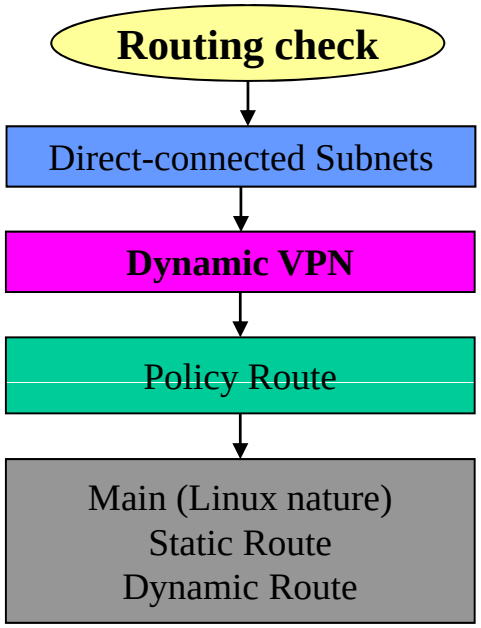
- **Problem on current ZLD 2.0x, 2.1x design**
  - Virtual Server problem
    - 1:1 mapping need to use policy route
    - NAT loop back need to use policy route
    - No many one to one support
    - If mapping IP is device unowned IP, device will create virtual interface for virtual server rule. (Need better solution)
  - Routing Issue
    - User need to create policy route for routing (e.g. lan traffic, wlan traffic)
    - Direct route always has higher priority than policy route
    - Set SNAT with device unowned IP on Policy Route is not work
  - Site to Site VPN need policy route

New Packet Flow Design

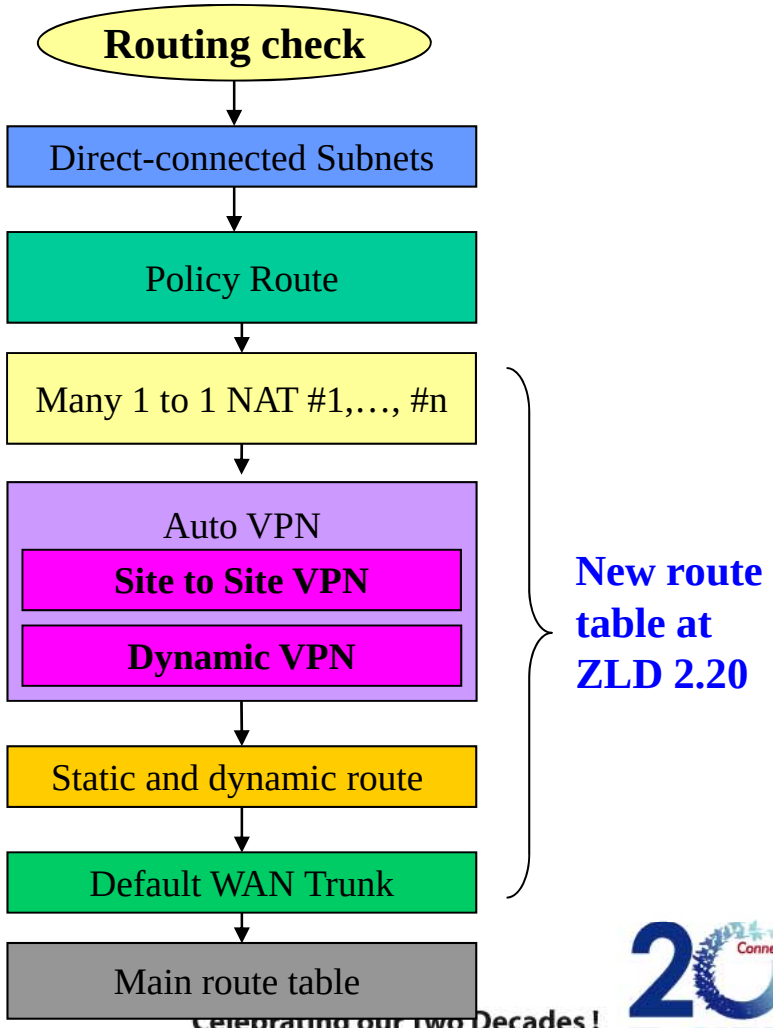
- **User do not need to set policy route for default LAN to WAN traffic and VPN traffic**
  - Default SNAT and WAN Trunk Routing
  - Static Route and Dynamic Route can be
  - Auto create VPN routing policy.
- **Support outgoing Many to Many NAT (Proxy ARP)**
- **New NAT loopback implementation**
- **Policy Route can be overwrite Direct Route**

ZLD Routing Table Changes

ZLD 2.1x design



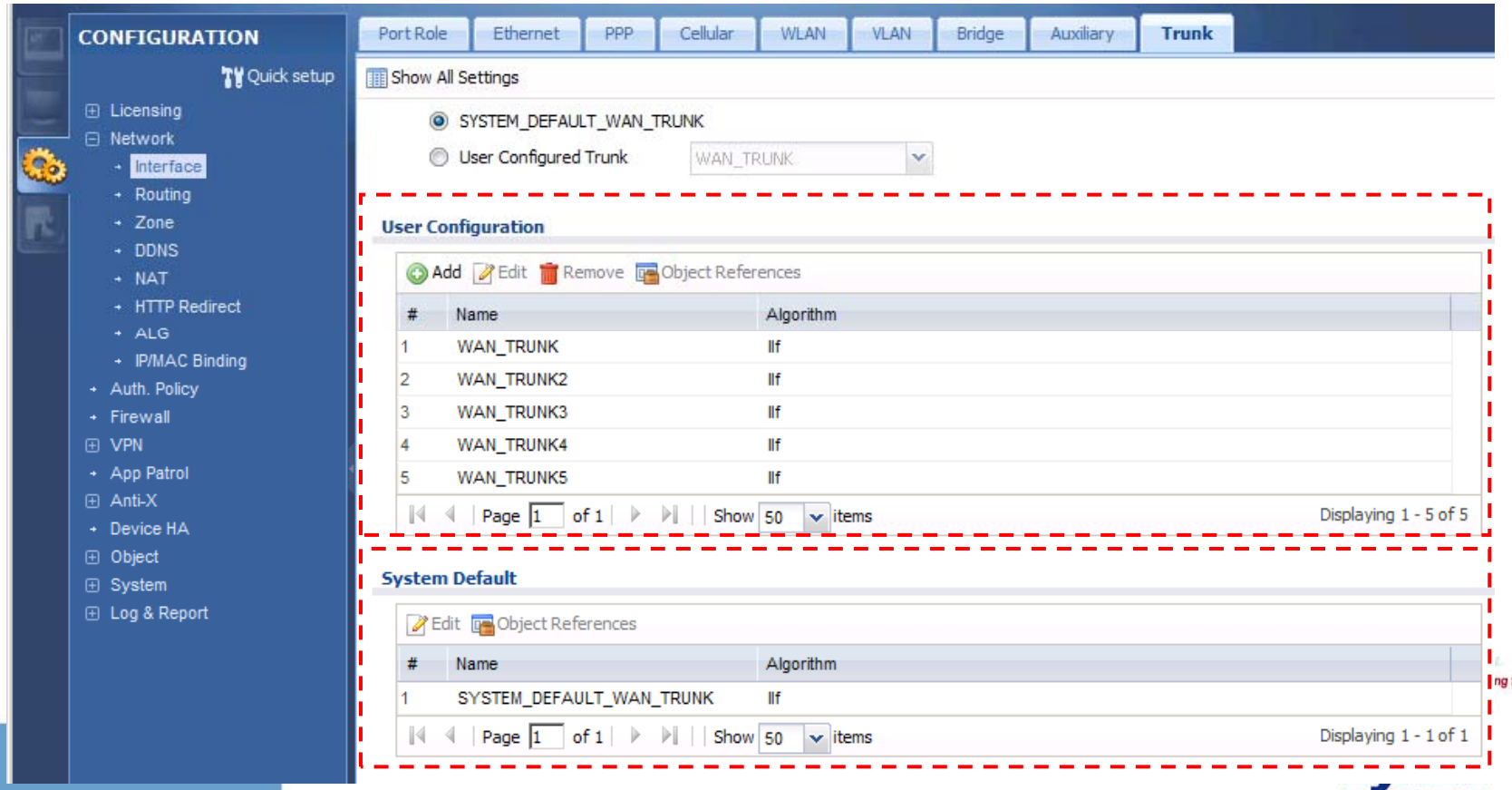
ZLD 2.20 design



Celebrating our Two Decades !
Connecting the Future !
ZyXEL

Default WAN Trunk

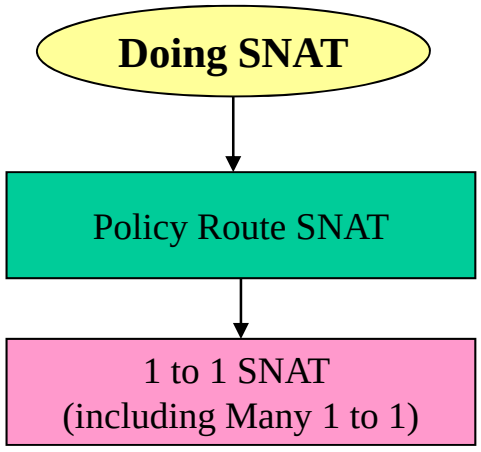
- Provide default Trunk “SYSTEM_DEFAULT_WAN_TRUNK” that user can not delete it.
- SYSTEM_DEFAULT_WAN_TRUNK will add external Ethernet interface and ppp/aux/cellular automatically



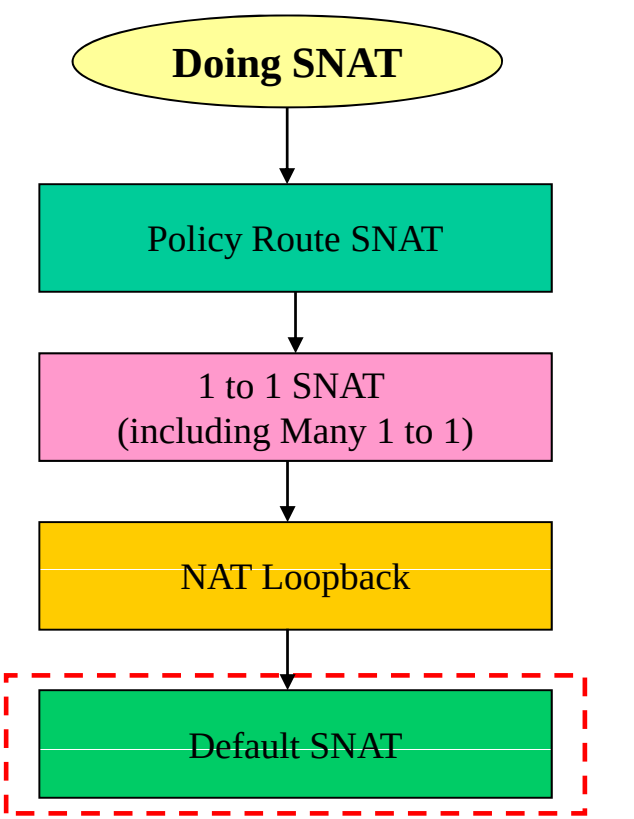
NAT Enhancement

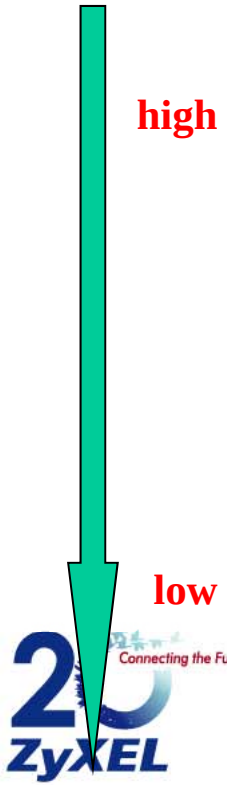
- Support 1 to 1 NAT and many 1 to 1 NAT
- New NAT loopback implementation
- NAT Table design change

ZLD 2.1x design



ZLD 2.20 design





Celebrating our Two Decades !

Default SNAT

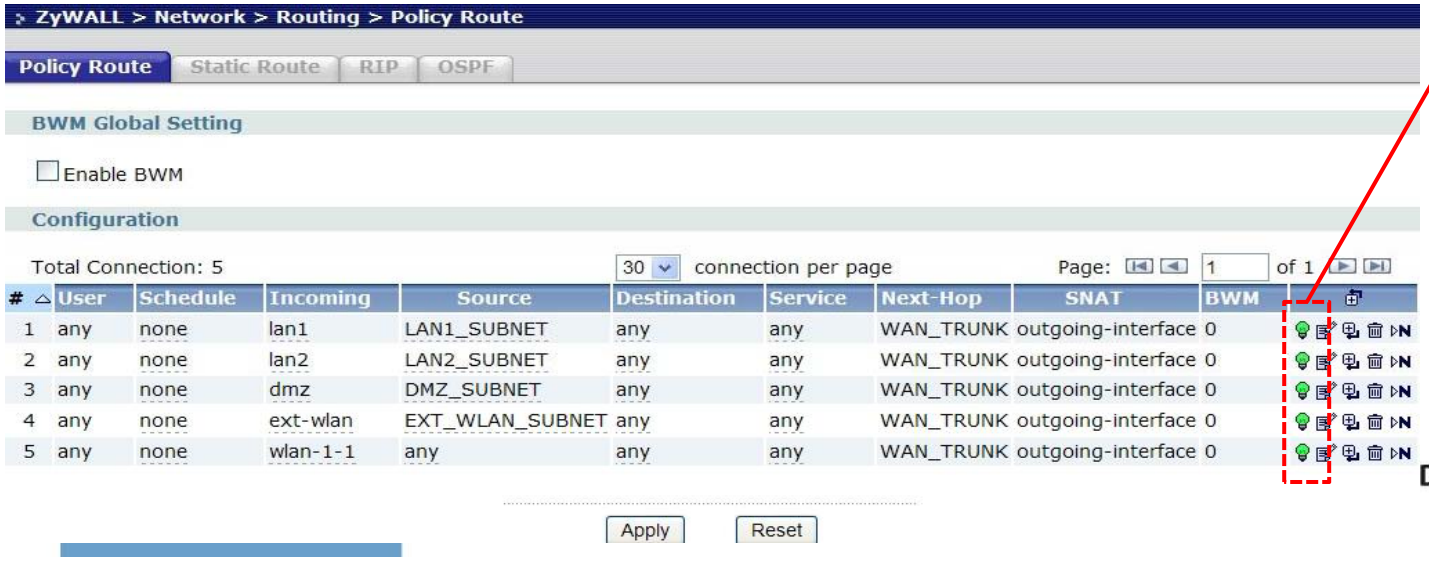
- Traffic that match the following criteria will do the related action.
- Only internal to external will do SNAT

	SNAT	Scenarios (Example)
Internal → external	On	LAN → WAN Access Internet
Internal → internal	Off	LAN → DMZ Access Server
external → Internal	Off	WAN → LAN Serving Internet access
external → external	Off	WAN → WAN Dynamic Route

Policy Route Enhancement

- **Goal**
  - Auto disable policy route when next hop is dead
- **Interface Status Base on**
  - Link up and down
  - Interface enable/disable
  - Connectivity check
  - Object IP or not

Activate (green)
Deactivate (gray)
Auto-Deactivated (red)


ZyWALL > Network > Routing > Policy Route
Policy Route
Static Route
RIP
OSPF
BWM Global Setting
Enable BWM
Configuration
Total Connection: 5
30 connection per page
Page: 1 of 1
User Schedule Incoming Source Destination Service Next-Hop SNAT BWM
1 any none lan1 LAN1_SUBNET any any WAN_TRUNK outgoing-interface 0
2 any none lan2 LAN2_SUBNET any any WAN_TRUNK outgoing-interface 0
3 any none dmz DMZ_SUBNET any any WAN_TRUNK outgoing-interface 0
4 any none ext-wlan EXT_WLAN_SUBNET any any WAN_TRUNK outgoing-interface 0
5 any none wlan-1-1 any any any WAN_TRUNK outgoing-interface 0
Apply
Reset

20 Decades ! Connecting the Future ! ZyXEL

Unified Interface Enhancement

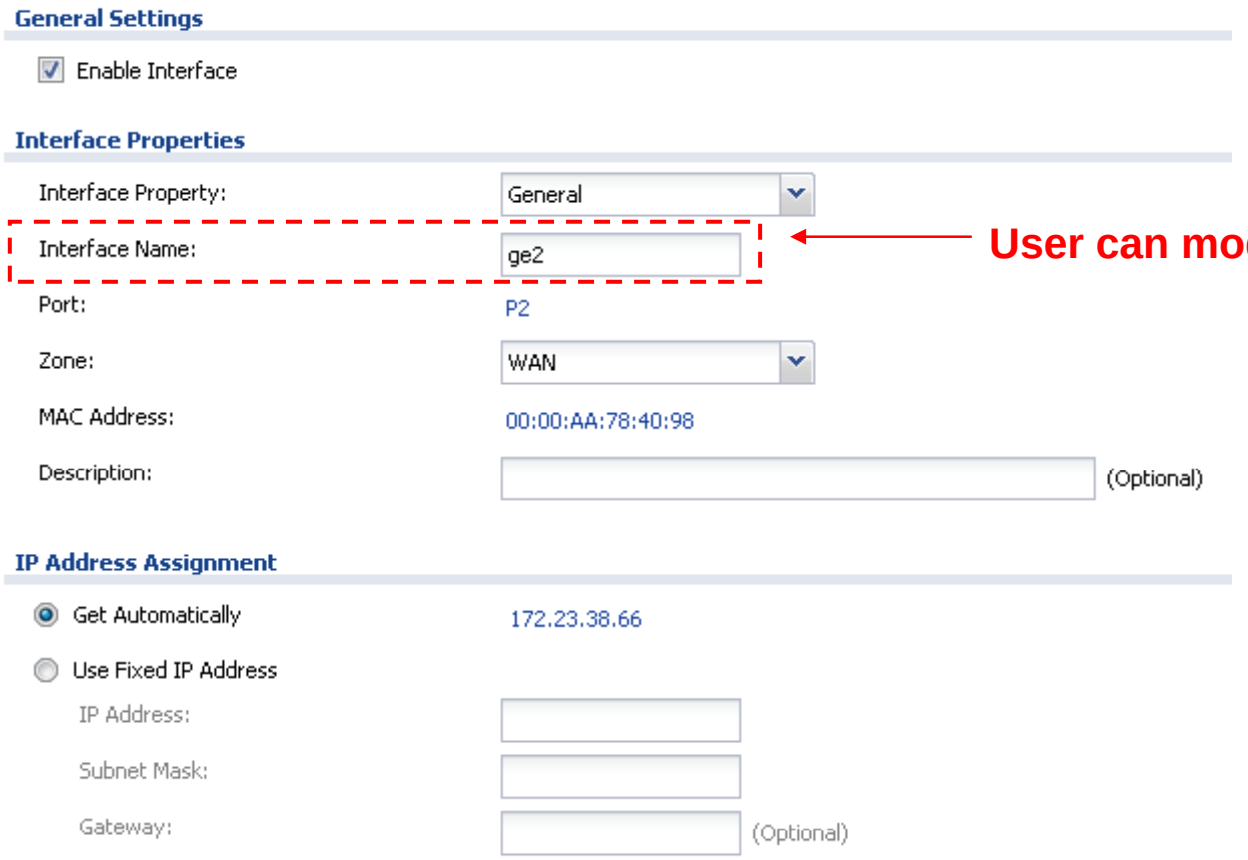
- **Purpose**
  - Provide more flexible and user friendly design
  - Make All USG Series have consistent Interface configuration style
- **Enhancement for ZLD 2.20**
  - Configurable Interface Name
  - Showing Port Information on Ethernet Interface
  - Interface Property
  - System Default PPP Interface
  - Zone/Trunk design change

Unify Interface Name for All Product

- **Before ZLD v2.20**
  - Interface name on USG100/200 device
    - wan1, wan2, opt, lan1, lan2, dmz
  - USG300/1000/2000, ZW1050
    - ge1, ge2, ge3 and so on
- **After ZLD 2.20**
  - Unify interface name design for all models
  - User can define a meaningful name

Configurable Interface Name (1/2)

- The interface name is configurable

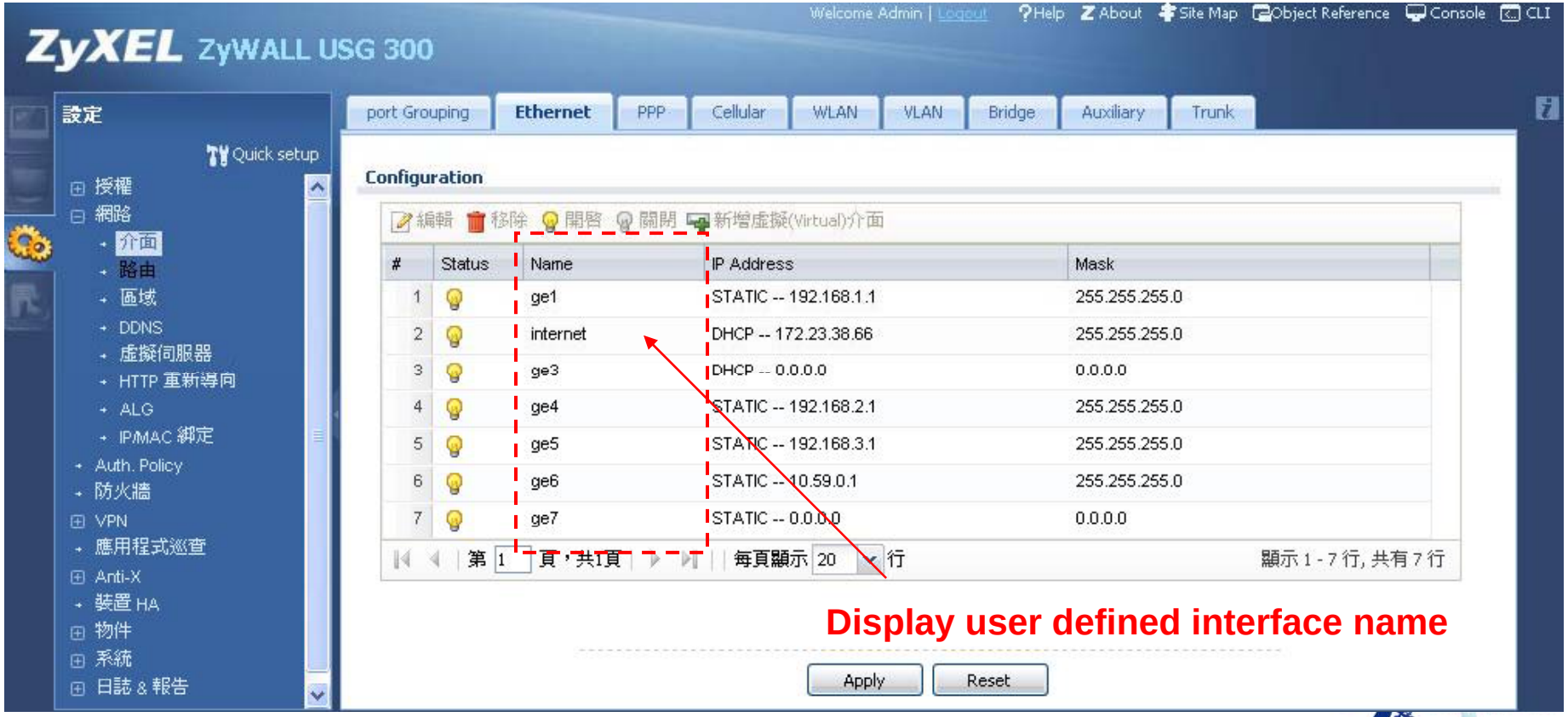


User can modify the interface name

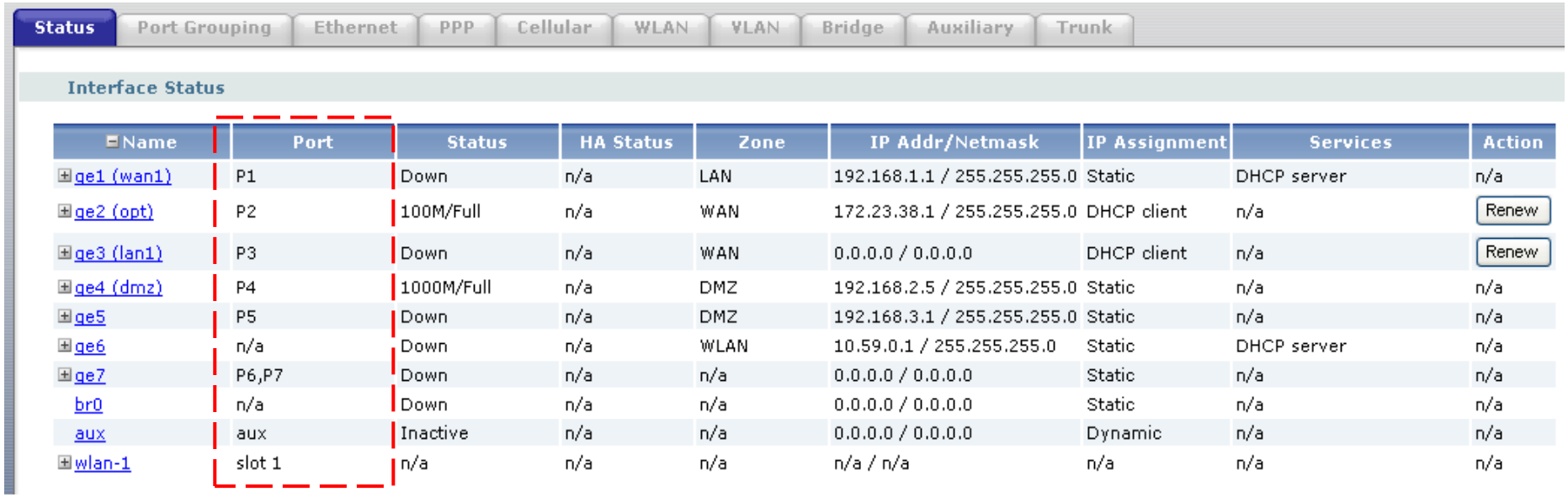
Celebrating our Two Decades !
Connecting the Future !
ZyXEL

Configurable Interface Name (2/2)

- New interface name will display at all features which using interface



Showing Port Information on Interface


Status
Port Grouping
Ethernet
PPP
Cellular
WLAN
VLAN
Bridge
Auxiliary
Trunk
Interface Status
Name
Port
Status
HA Status
Zone
IP Addr/Netmask
IP Assignment
Services
Action
ge1 (wan1) P1 Down n/a LAN 192.168.1.1 / 255.255.255.0 Static DHCP server n/a
ge2 (opt) P2 100M/Full n/a WAN 172.23.38.1 / 255.255.255.0 DHCP client n/a Renew
ge3 (lan1) P3 Down n/a WAN 0.0.0.0 / 0.0.0.0 DHCP client n/a Renew
ge4 (dmz) P4 1000M/Full n/a DMZ 192.168.2.5 / 255.255.255.0 Static n/a n/a
ge5 P5 Down n/a DMZ 192.168.3.1 / 255.255.255.0 Static n/a n/a
ge6 n/a Down n/a WLAN 10.59.0.1 / 255.255.255.0 Static DHCP server n/a
ge7 P6,P7 Down n/a n/a 0.0.0.0 / 0.0.0.0 Static n/a n/a
br0 n/a Down n/a n/a 0.0.0.0 / 0.0.0.0 Static n/a n/a
aux aux Inactive n/a n/a 0.0.0.0 / 0.0.0.0 Dynamic n/a n/a
wlan-1 slot 1 n/a n/a n/a n/a / n/a n/a n/a n/a

Interface	***Display wording***
Ethernet: ge1(wan1), ge2(wan2), ge3(lan1)…	P1, P2, P3,…
VLAN, PPP	Display it's base physical port, such as P1, P2…
Bridge	n/a
WLAN, Cellular	Display the location it is, such as shot1/shot2 or USB1/USB2
Aux	aux

Celebrating our Two Decades !
Connecting the Future !
ZyXEL

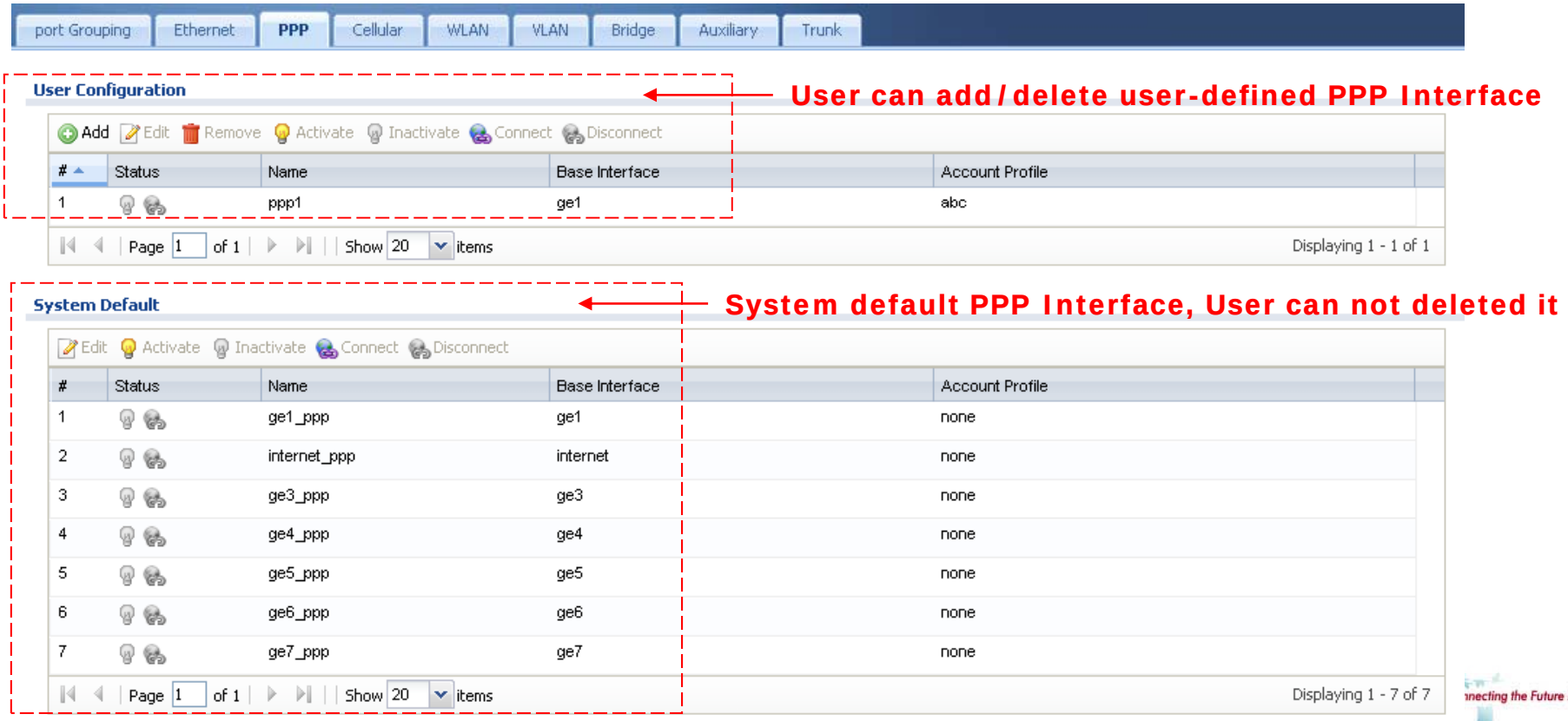
Interface Property

- Differentiate interface into several groups
- Different setting for different property
  - To simplified configuration page on GUI

Type	Internal	External	General
Device Model	USG 100/200: LAN1, LAN2, DMZ	USG 100/200: WAN1, WAN 2	USG 300/1000/2000: ge1, ge2...
Set DHCP Client	Not Support	Support	Support
Set DHCP Server	Support	Not Support	Support
Set DHCP Relay	Support	Not Support	Support
Set Default Gateway	Not Support	Support	Support
Set Metric	Not Support	Support	Support
Set Ping Check	Not Support	Support	Support
MAC Address Setting	Not Support	Support	Support

System Default PPP Interface

- Support binding multiple PPP interfaces in one WAN interface for USG 100/200 .
- Support setup PPP on VLAN interface for USG 100/200.



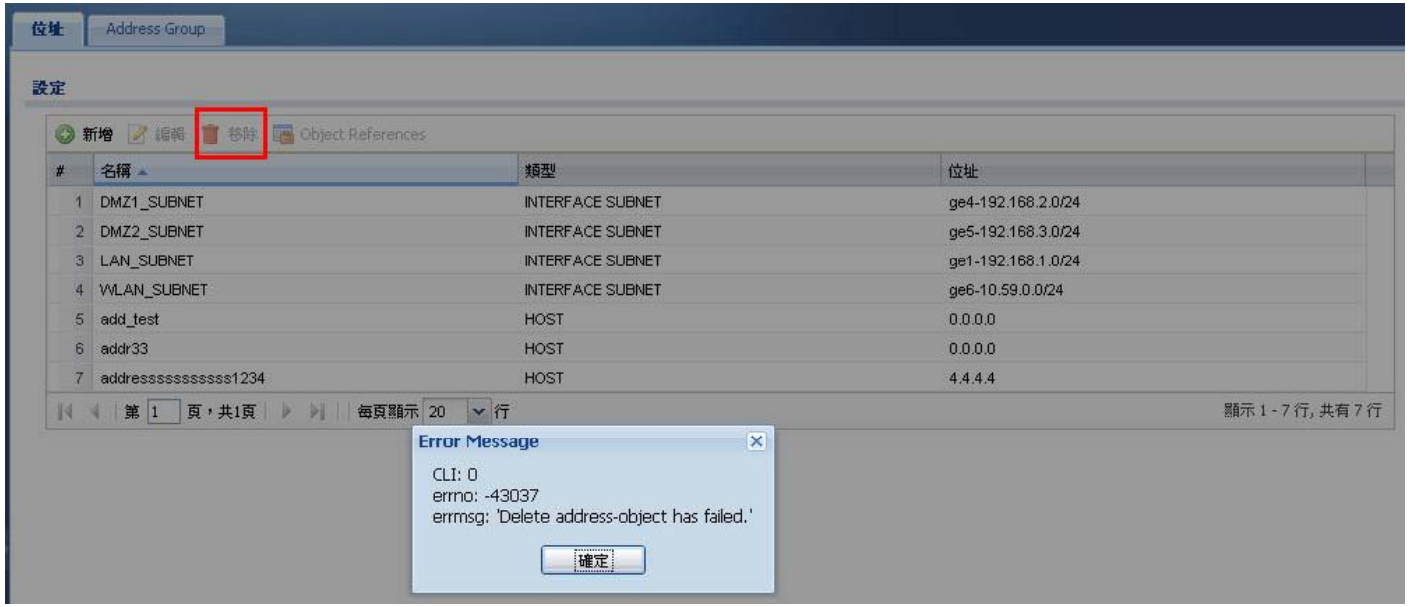
Celebrating our Two Decades !
ZyXEL

Zone/Trunk design change

Type	Before ZLD v2.20	After ZLD v2.20
ZONE		
USG 100/200	a. Fixed ZONE: - WAN, - LAN1, - LAN2, - WLAN, - DMZ, - OPT(only for USG200), - SSL_VPN, - IPSec VPN b. User can not create/delete ZONE.	a. System default ZONE: - WAN, - LAN1, - LAN2, - WLAN, - DMZ, - OPT(only for USG200), - SSL_VPN, - IPSec VPN b. User can create/delete ZONE
USG 300/1000/2000	User can create/delete ZONE.	
TRUNK		
USG 100/200	a. Limit to 5 TRUNK : -WAN_TRUNK, -WAN_TRUNK2, -WAN_TRUNK3, -WAN_TRUNK4, -WAN_TRUNK5 b. User can not add /delete existent TRUNK	a. No Limitation of Fixed 5 TRUNKs b. User can add/delete TRUNK
USG 300/1000/2000	User can add/delete TRUNK	

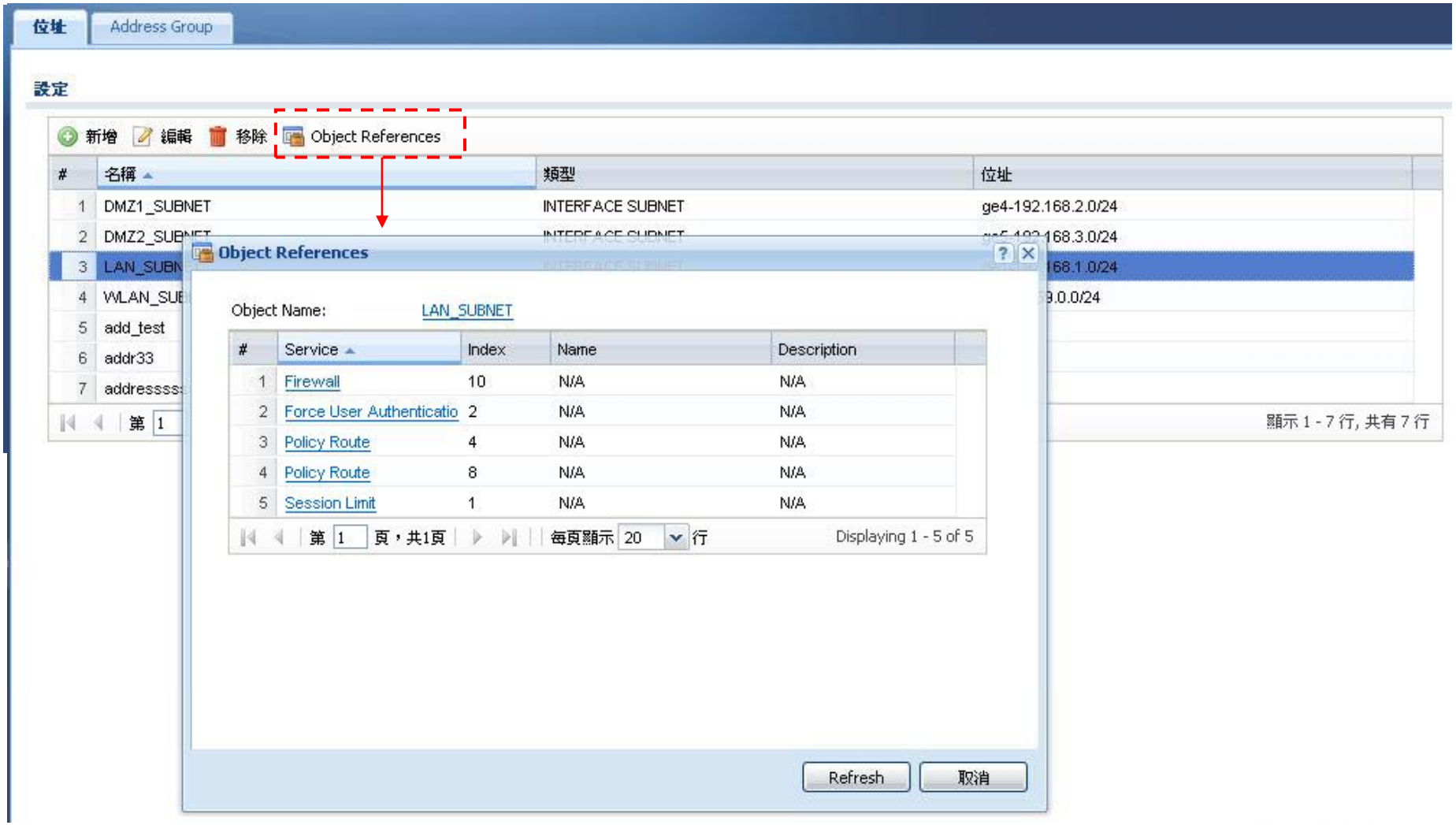
Object Reference

- **Current issue:**
  - When user try to remove an used object, the system will return failed message, but no further information.



- **New design:**
  - A mechanism to get all references for Object/Group.

Object Reference: GUI



Celebrating our Two Decades !
Connecting the Future !
20 ZyXEL

CF Enhancement

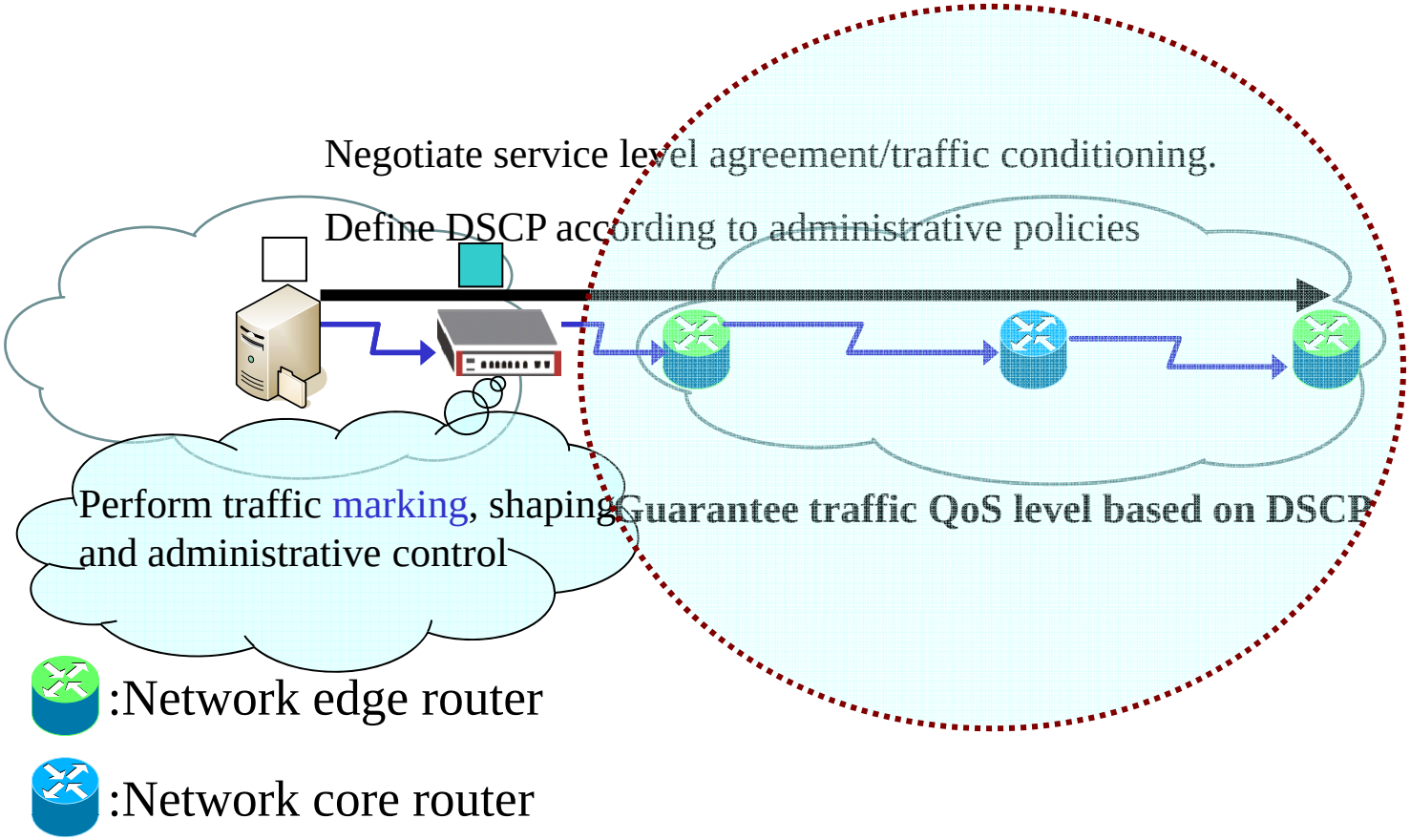
- Some user request not to do content filter checking when passing thru VPN tunnel
- Add a CLI command to Bypass/Inspect CF filter on VPN traffic

BWM

- Diff SERV tagging
- BWM by DSCP mark

Celebrating our Two Decades !

What DiffServ Code Point is?


Negotiate service level agreement/traffic conditioning.
Define DSCP according to administrative policies
Perform traffic marking, shaping and administrative control
Guarantee traffic QoS level based on DSCP
:Network edge router
:Network core router

DSCP Design

- **Objective**
  - DSCP-aware traffic conditioning, shaping and marking
  - Support DSCP marking based on application layer
- **DSCP functionality in ZLD**
  - Marking: classify traffic to different DSCP value according to application or source/destination IP, service and even user-aware
  - Bandwidth management: packets with different DSCP will receive differentiated BWM
  - Routing: different DSCP tagged packets can get distinct routing result or NAT
- **Combine DSCP control into policy rule and App. Patrol**

End point security

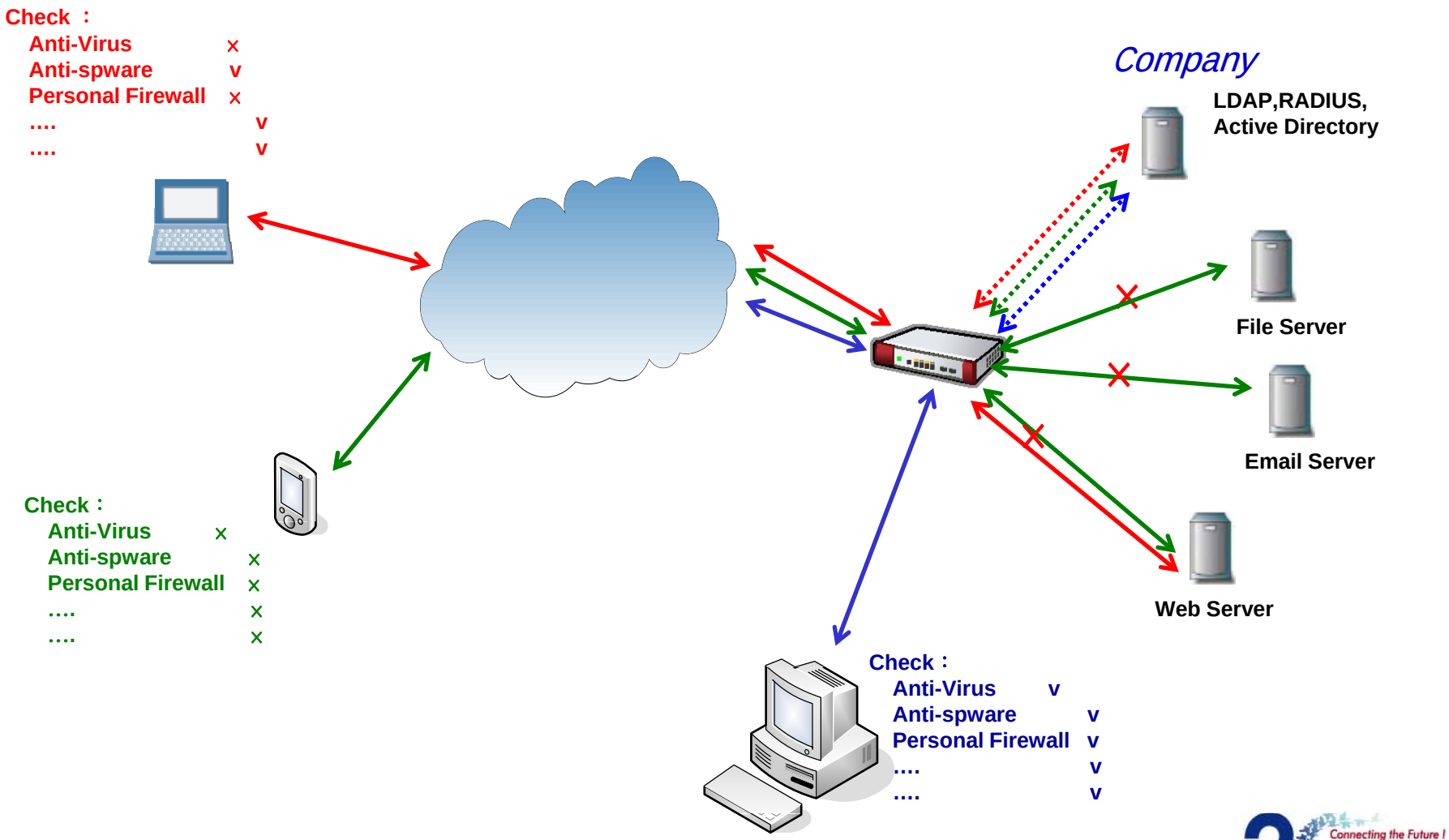
- **EPS with SSL VPN**
- **EPS with Authentication Policy**

Celebrating our Two Decades !

EPS with SSLVPN

- **Security software is distributed to end-user devices.**
- **A program is downloaded and installed on endpoint and checks endpoint security status when endpoint access controlled by ZyWALL.**
- **If endpoint operation environment matches company security requirement, the access will be granted.**
- **Check Client Host for**
  - Anti-Virus Installation & Activation
  - Anti-Spyware Installation & Activation
  - Personal Firewall Installation & Activation
  - User define checking on OS internal setups. Ex: Windows Registry.

Scenario with EPS checking



Celebrating our Two Decades !

EPS with Authentication Policy

- Improving Version of Force User Authentication
- Network Admission Control.
- Do EPS checking after user authentication.
- User can access network after pass User authentication and EPS checking.

ZyXEL

Windows 7 ready

- SSL VPN enhancement

Connecting the Future !

Celebrating our Two Decades ! ZyXEL

Support Windows 7

Technical elements/Spec	Top-down road map			Note
	(4Q'09)	(1Q'10)	(2Q'10)	
	ZLD 2.12 patch x	**ZLD 2.20**	**ZLD 2.21**	
SSLVPN Full tunnel: Run SecuExtender in Windows 7	yes	yes	yes	
SSLVPN Proxy mode: User run IE8 in Windows 7	yes	yes	yes	
Device Management: Administrator use IE8 in Windows 7	yes	yes	yes	
EPS: Set poilcy to detect Windows 7	no	yes	yes	
	(4Q'09)	(2Q'10)	(4Q'10)	
IPSec VPN client (TGB)	yes	yes	yes	IPSec version: 2.4.204.61.03

Celebrating our Two Decades !
Connecting the Future !
ZyXEL

ZyXEL

Better Look n' Feel

- GUI 2.0

Connecting the Future !

Celebrating our Two Decades ! ZyXEL

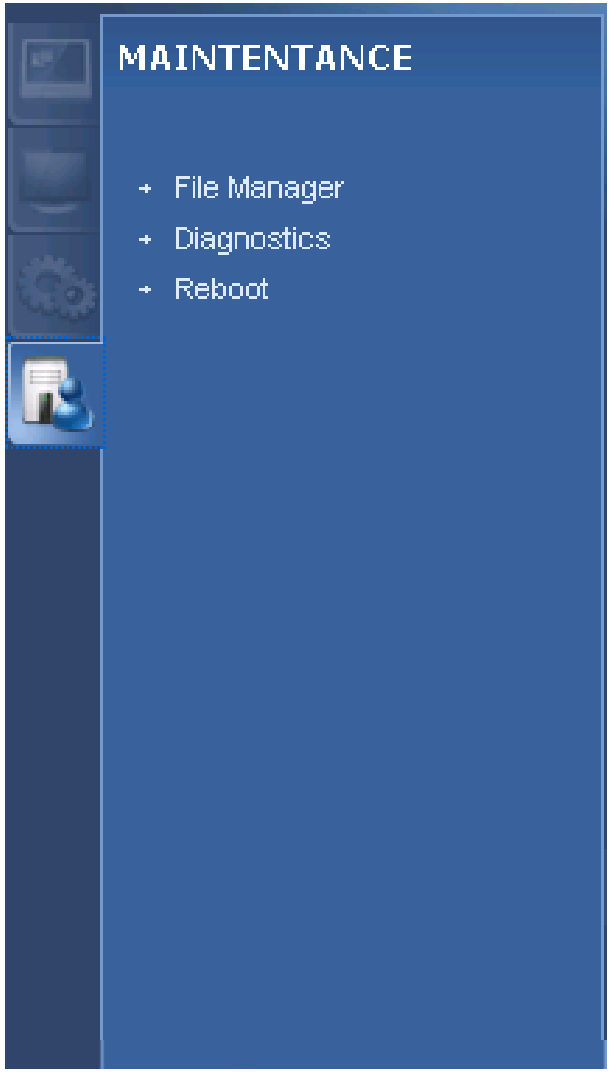
Web GUI 2.0 Introduction

- **ZLD Web GUI 2.0 is based on Ext-JS's library to develop because of**
  - High performance, customizable UI widgets
  - Well designed, documented and extensible component model
  - Well browser compatibility

Web GUI 2.0 Property

- **Reorganized Menu Tree**
- **Easy to monitor device status**
  - Virtual Device
- **Customizable dashboard**
- **User Friendly Table Operation**
  - More user-friendly interface to configure

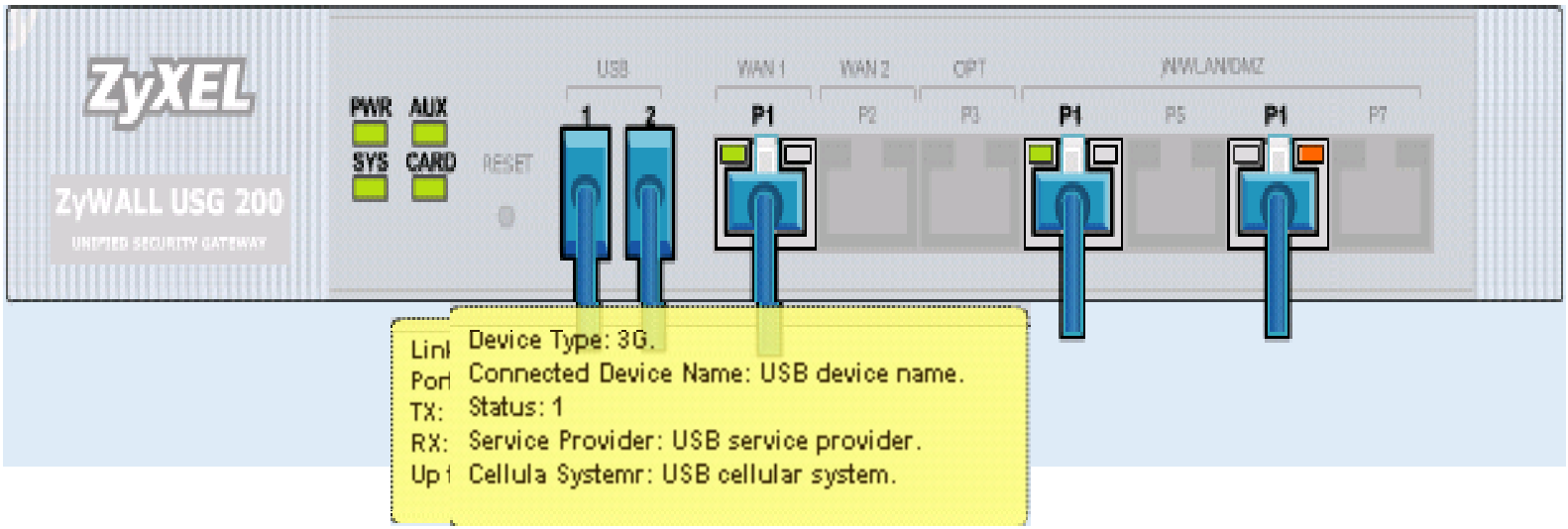
Reorganized Menu Tree



- Dash Board
- Monitor
- Configuration
- Maintenance

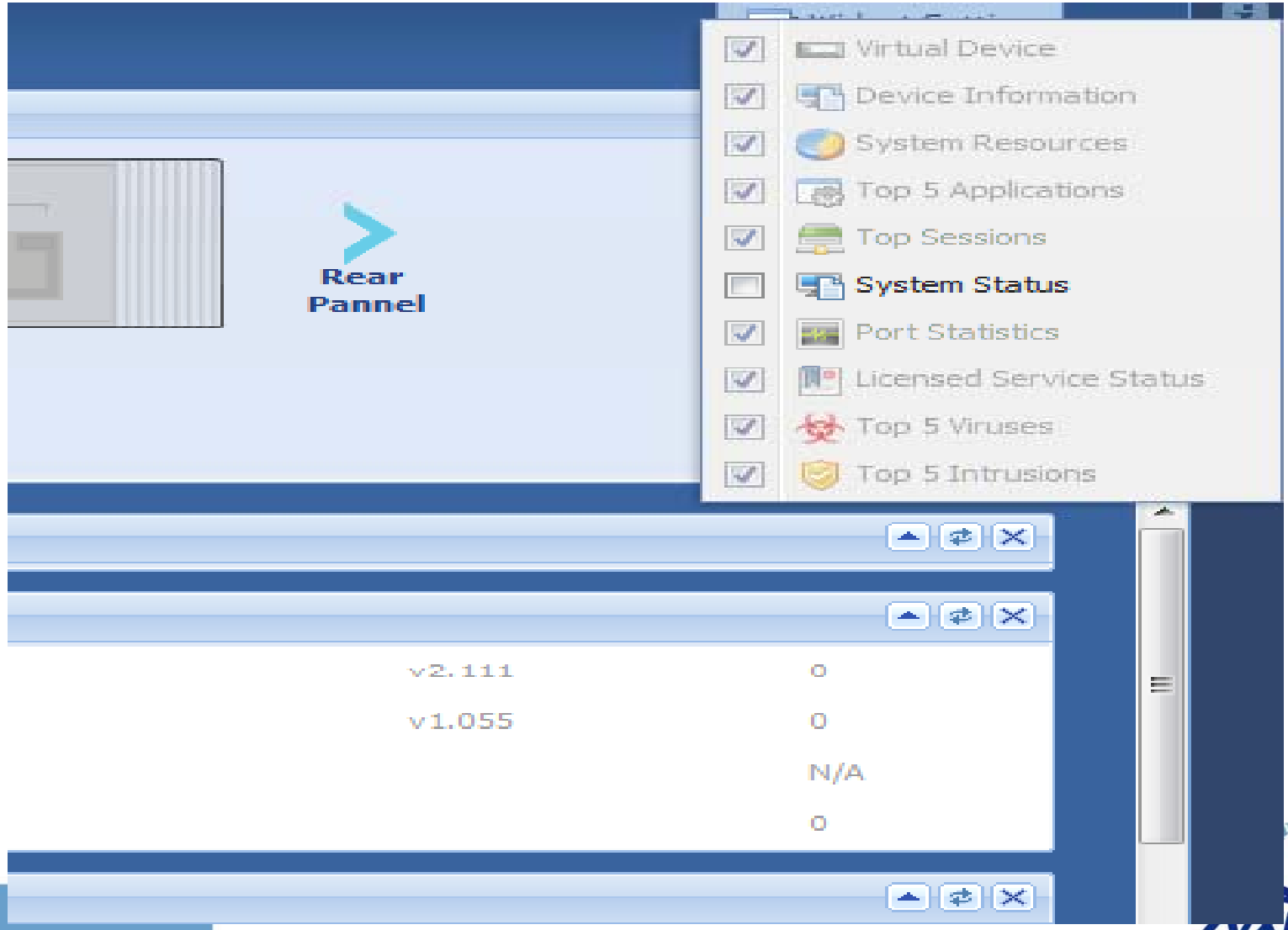
Celebrating our Two Decades !
Connecting the Future !

Virtual Device



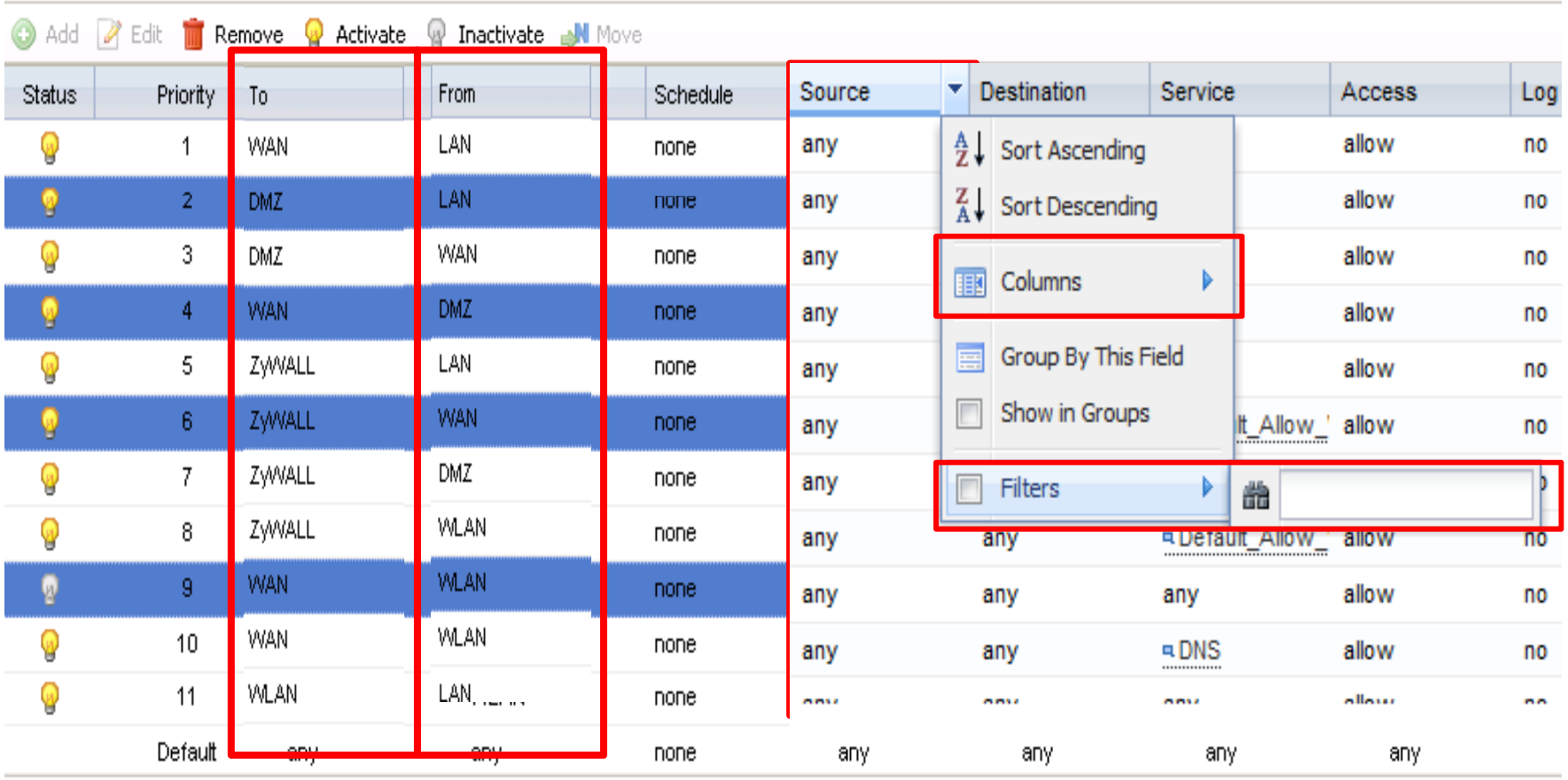
Customized Dashboard (1/2)

Customized Dashboard (2/2)



Connecting the Future !

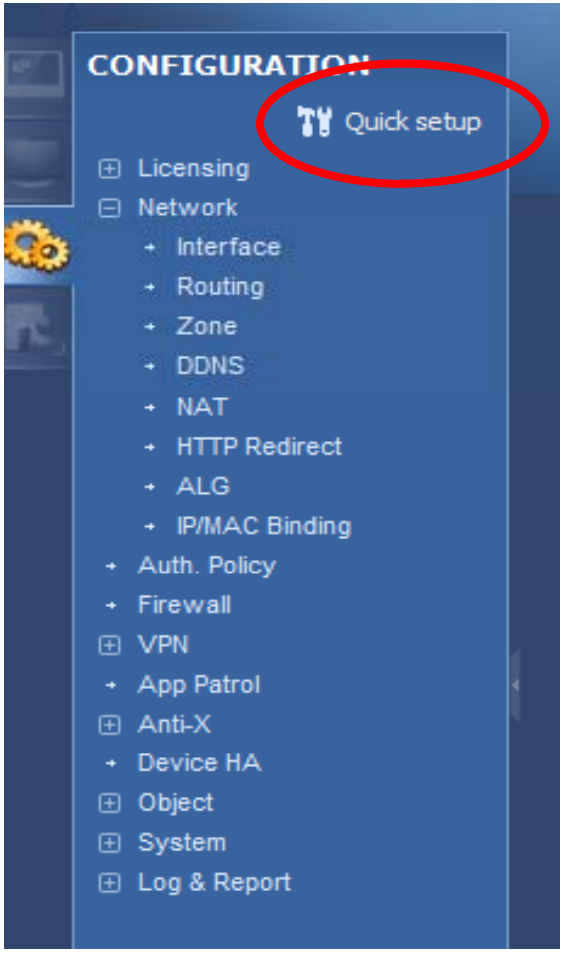
User Friendly Table Operation

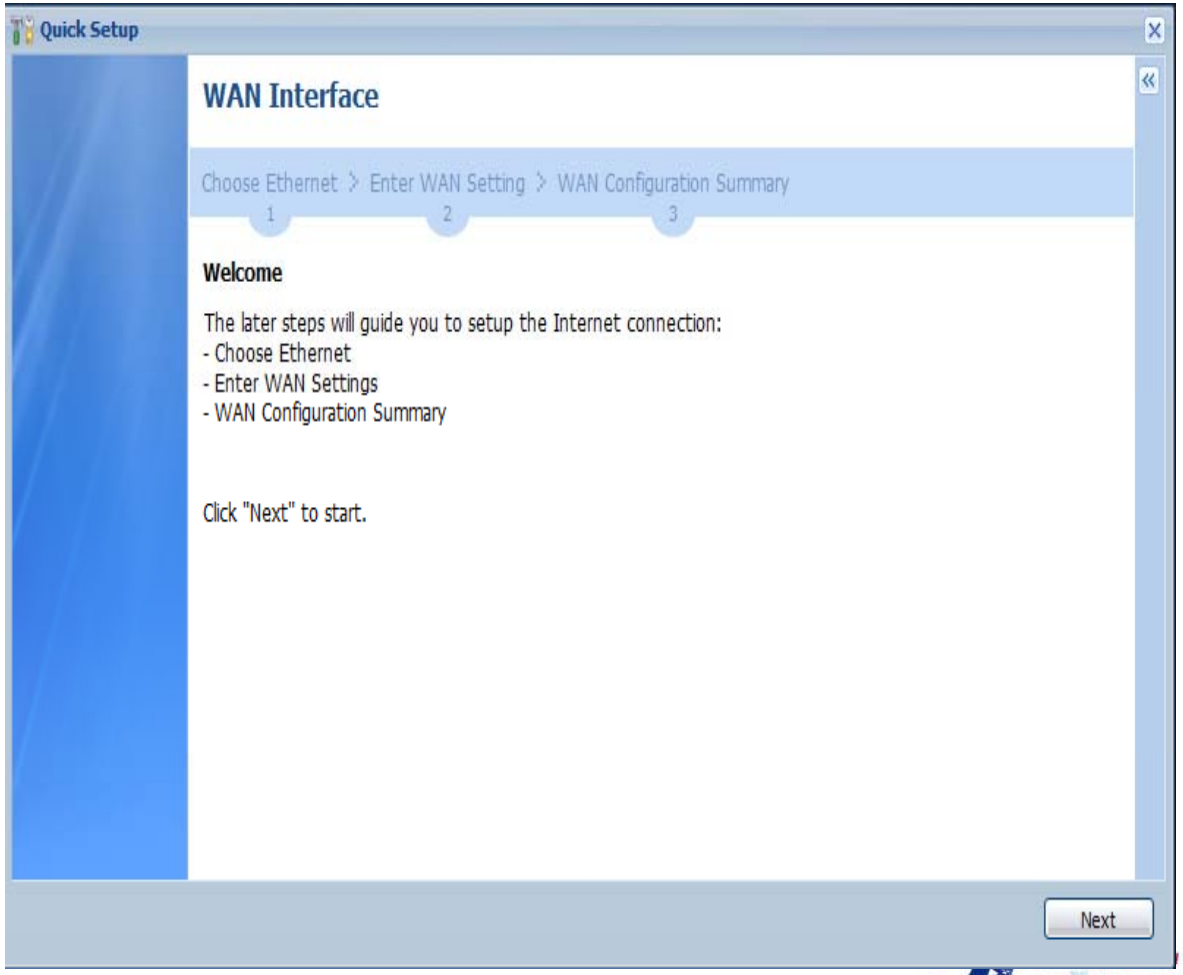


Celebrating our Two Decades !

Connecting the Future !

Quick Setup


CONFIGURATION
Quick setup
Licensing
Network
Interface
Routing
Zone
DDNS
NAT
HTTP Redirect
ALG
IP/MAC Binding
Auth. Policy
Firewall
VPN
App Patrol
Anti-X
Device HA
Object
System
Log & Report


Quick Setup
WAN Interface
Choose Ethernet > Enter WAN Setting > WAN Configuration Summary
1
2
3
Welcome
The later steps will guide you to setup the Internet connection:
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary
Click "Next" to start.
Next

Trouble shooting made easy

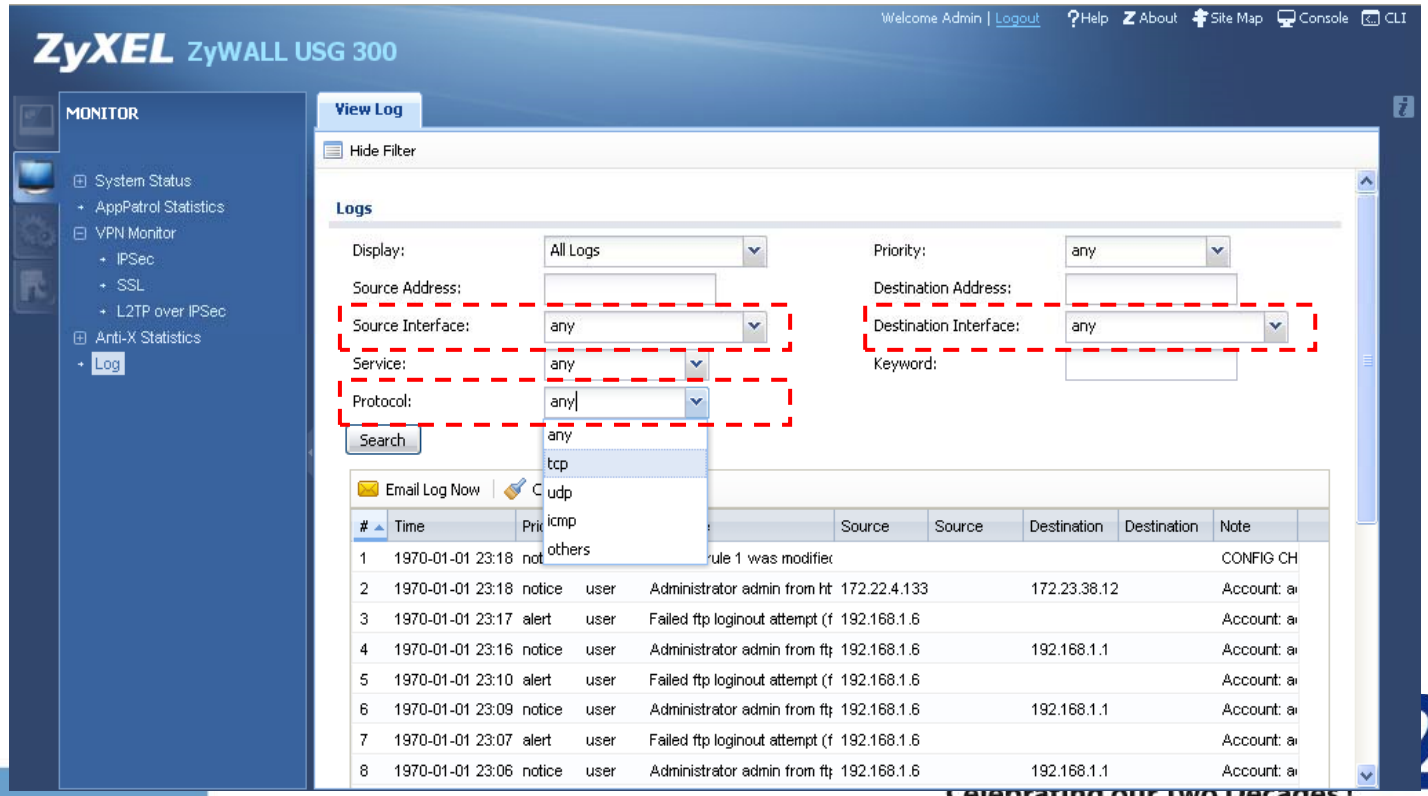
- LOG in GUI 2.0
- Debug Tool

Connecting the Future !

Celebrating our Two Decades !

LOG

- **Support extra log column**
  - Source interface
  - Destination interface
  - Protocol



Connecting the Future !
Celebrating our Two Decades !
ZyXEL

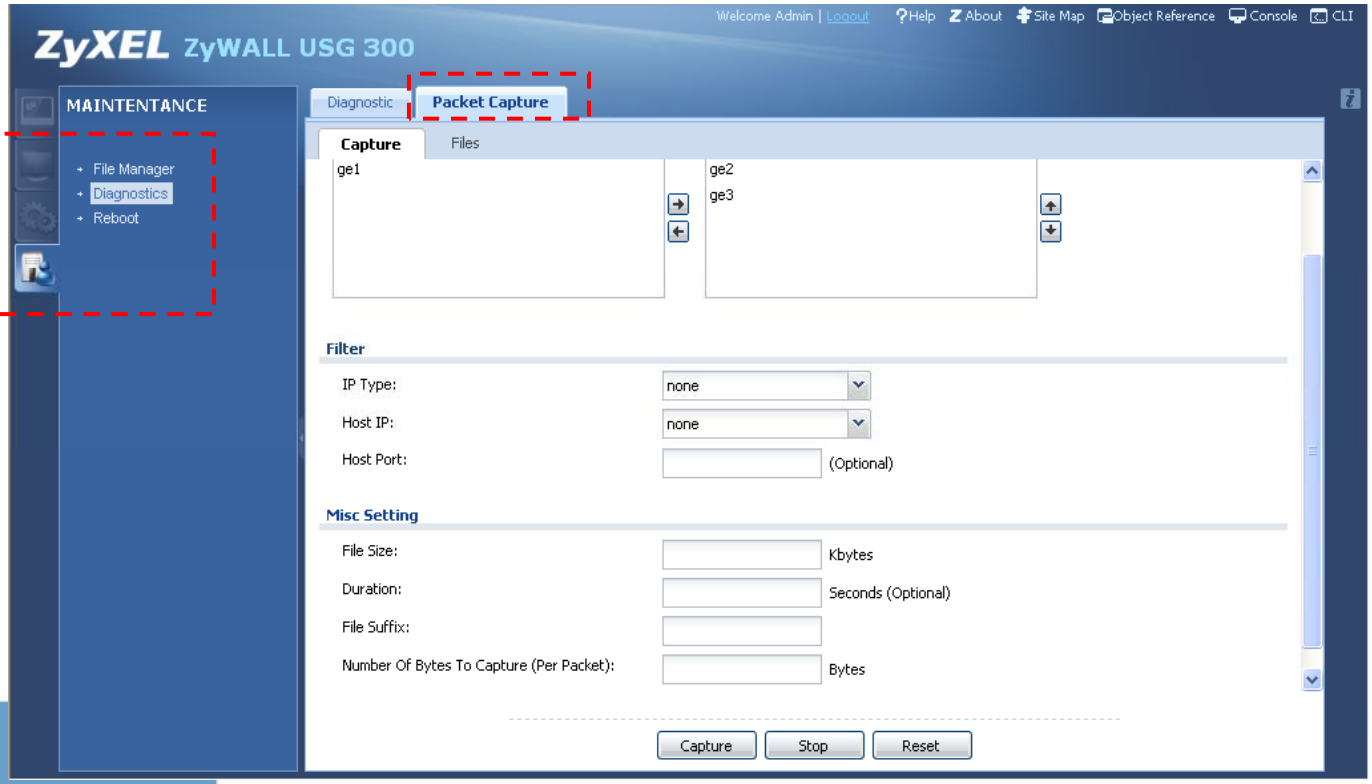
APP Patrol Enhancement

- **Support log MSN user login/logout**
  - MSN user XXX has logged in.
  - MSN user XXX has logged out.

#	Time	Priority	Category	Message	Sou
1	2009-03-18 07:45:04	alert	Application Patrol	MSN:User zyxelstan@livemail.tw has logged out!	192.168
2	2009-03-18 07:44:34	notice	User	Administrator admin from http/https has logged in ZyWALL	192.168
3	2009-03-18 07:44:31	alert	Application Patrol	MSN:User zyxelstan@livemail.tw has logged in!	192.168
4	2009-03-18 07:44:29	alert	Application Patrol	Service=msn Mode=port-less Rule=1 Access=forward	192.168
5	2009-03-18 07:44:28	alert	Application Patrol	Service=msn Mode=port-less Rule=1 Access=forward	192.168
6	2009-03-18 07:43:21	notice	User	Administrator admin from console has logged out ZyWALL	
7	2009-03-18 07:43:06	notice	User	Administrator admin from console has logged in ZyWALL	
8	2009-03-18 07:42:36	info	Policy Route	ZyWALL USG 300 is configured successfully with startup configuration file.	
9	2009-03-18 07:42:35	notice	Application Patrol	Rule msn:1 has been modified	
10	2009-03-18 07:42:35	info	Application Patrol	Default port 1863 of service msn has been added.	
11	2009-03-18 07:42:35	info	Application Patrol	Default port 554 of service rtsp has been added.	
12	2009-03-18 07:42:35	info	Application Patrol	Default port 5060 of service sip has been added.	

Debug tool

- Make it easy for trouble shooting
- Support GUI page for packet capture.
- Support multiple interface packet captures.
- Download the packet capture result from GUI.



ZyXEL

Misc

Connecting the Future !

Celebrating our Two Decades ! ZyXEL

AAA Enhancement

- **In ZLD current design, grouping of external users is not user-friendly.**
  - Use a big group (i.e. ldap-users) to represent all external users.
  - User-defined group members MUST be manually-keyed in.
- **New design is going to:**
  - Instead of using a container to contain thousands of users, use a user to represent them.
  - Support as many as scenarios as possible.
  - Need as few as configuration steps as possible.

AAA Enhancement - Design Coverage

- **This enhancement is only applied to those services support both external AAA and user-aware.**
  - Services supporting external AAA can authenticate users by external AAA server.
    - weblogin, L2TP, x-auth, WLAN
  - Services supporting user-aware notify user-aware feature about user login/logout status.
    - weblogin, dialin, ftp, login, ssh
  - From now on, only weblogin case will be focused.

Budget Control: 3G

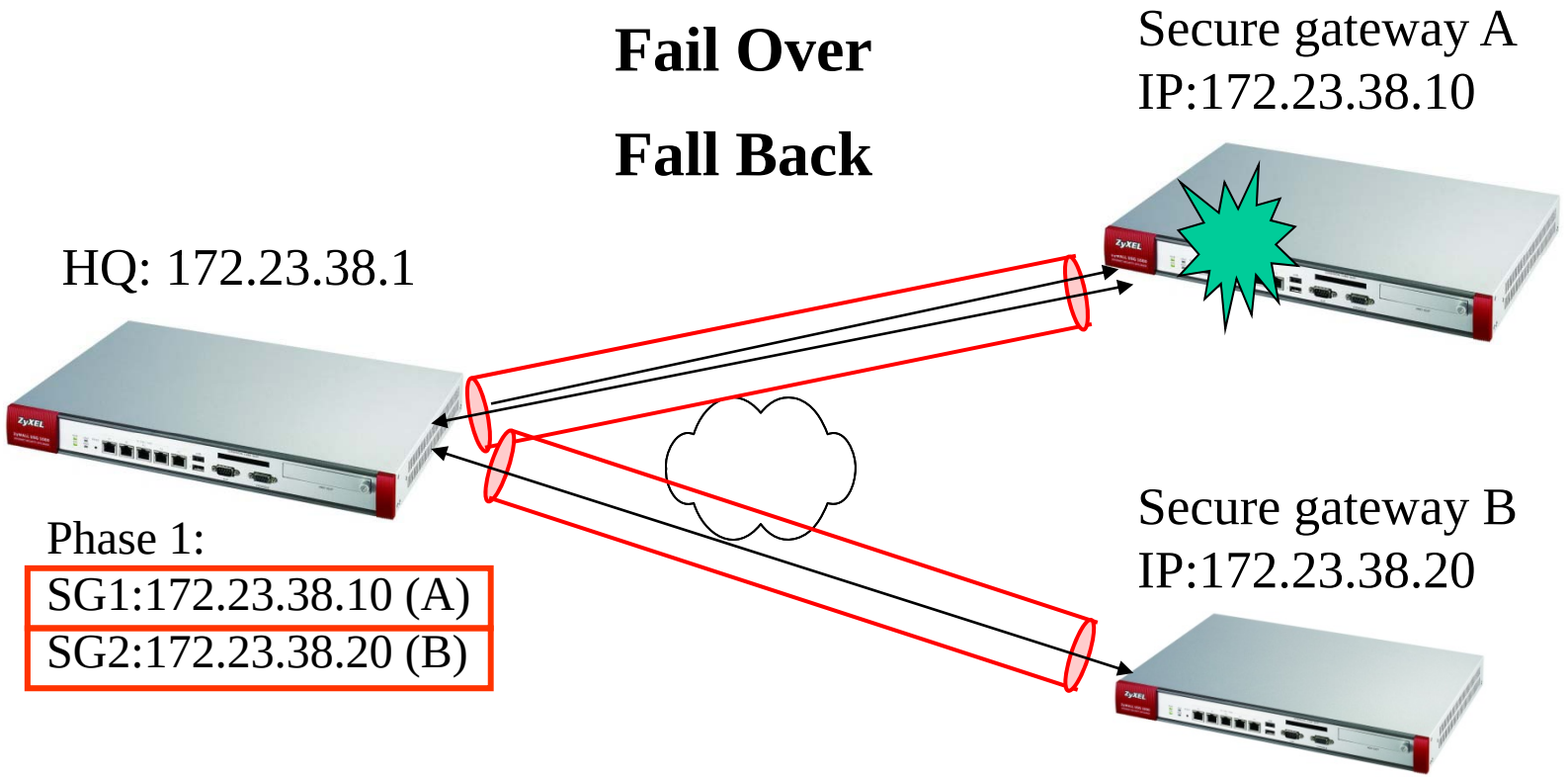
- **Control 3G network usage by**
  - Time Usage
  - Data Transmit
- **Action supports**
  - Log/Alert
  - Connection Dropped

Celebrating our Two Decades !
Connecting the Future !
20 ZyXEL

IPSec VPN: Fall Back

- Fail Over: Negotiate tunnel with secondary remote gateway when primary remote gateway is dead
- Fall Back: Let tunnel re-connect to primary remote gateway, even if secondary remote gateway is alive
- If secondary remote gateway is alive then it always keep connection with secondary because of IPSec daemon record the dead remote gateway

IPSec VPN: Auto Fall Back



No Fail Over ➔ No Fall Back
Fall Back ➔ Fail Over

Celebrating our Two Decades !
Connecting the Future !
20 ZyXEL

Device HA Enhancement

- Supports VLAN and Bridge interface on Device HA AP Mode
- Device HA backup will not doing NTP Sync (ITS)

SIP ALG 1.2

- **Purpose: Support IPPBX in DMZ zone scenario**
- **Design coverage:**
  - Ports SIP Tracking
    - Listening UDP ports on SIP: max 8 ports
  - Behaviors:
    - Related SIP connections
      - Help APP Patrol to monitor sip connection
    - NAT ALG
      - Modify packets under NAT environment
      - Help clients to construct media connection under NAT environment
    - Extend SIP connections' lifetime
  - Customized controls

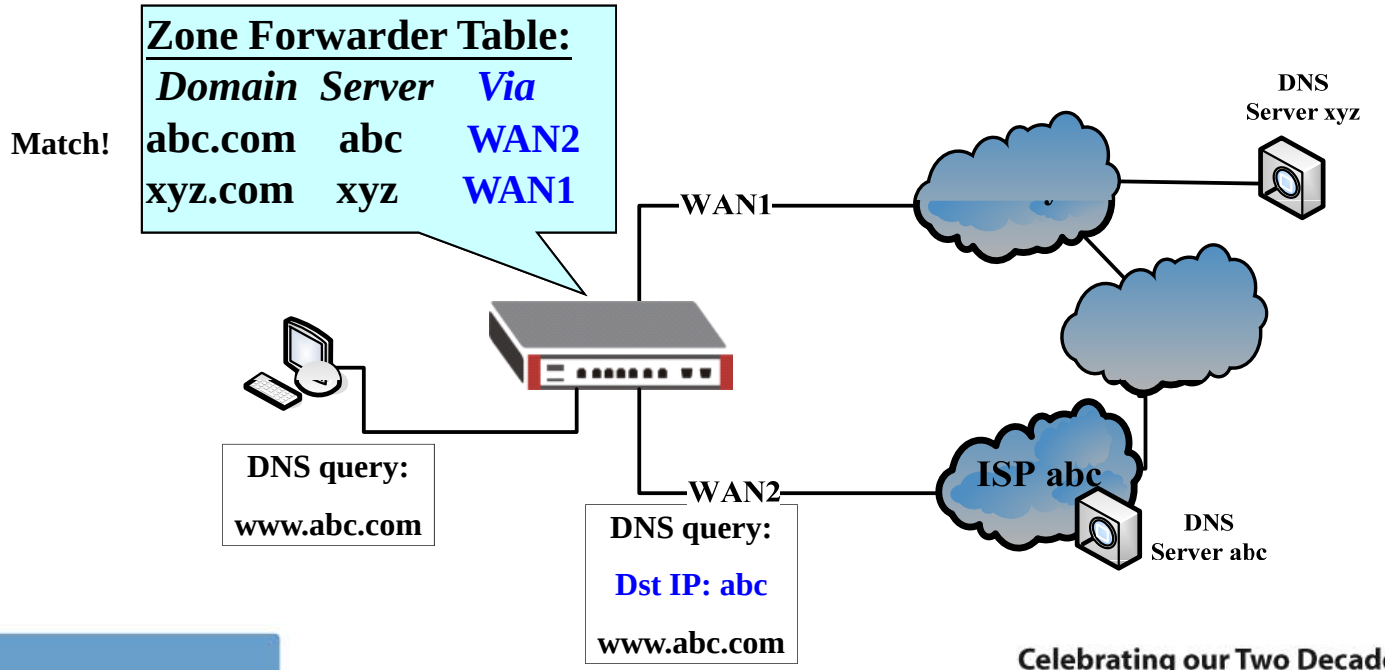
DNS Query Enhancement (1/2)

Current problem:

- **The destination DNS server of zone forwarder is decided by domain of inquired FQDN**
- **Problem**
  - Routing entries determines the interface from which DNS query will be sent out
  - DNS query will be dropped if destination DNS server requires DNS query must be came from its ISP network
- **Some DNS queries with specific domain need to be bound to specific interface**

DNS Query Enhancement (2/2)

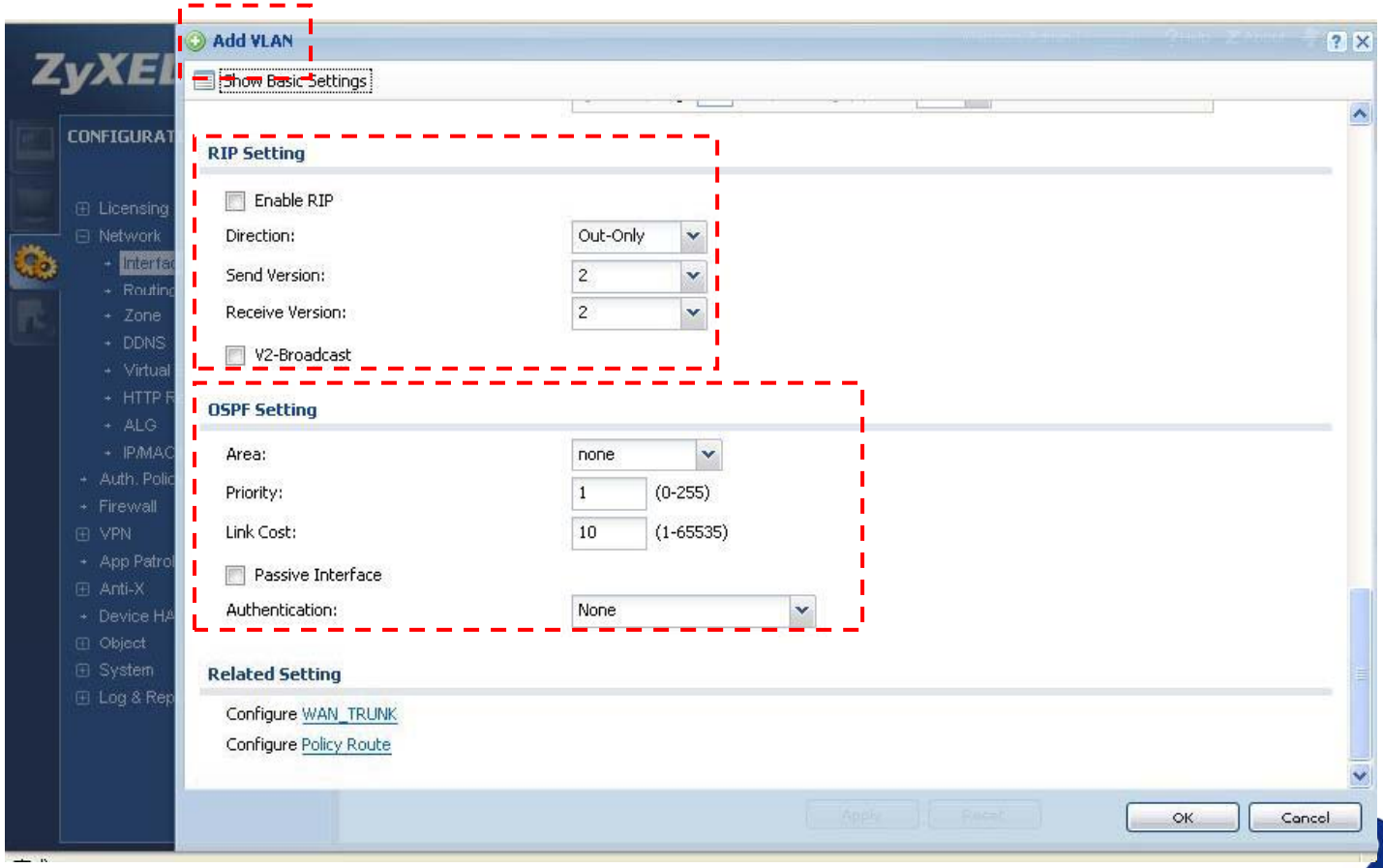
- **Force DNS query packet to be bound with specific interface when send it out**
  - **interface name** (ge1, ge2 ..)：DNS server from ISP or customized DNS server. DNS query will be bound to the configured interface
  - **any**：Customized DNS Server. Outgoing interface for DNS query depends on routing decision
  - **tunnel**：DNS server at remote network. DNS query will pass through tunnel



Celebrating our Two Decades !

RIP/OSPF enhancement

- When edit VLAN, user could setup RIP/OSPF



ZyXEL

FAQ

Connecting the Future !

Celebrating our Two Decades ! ZyXEL